UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/006,743	12/04/2001	Jonathan James Stone	450110-03698	2606

20999   7590   06/06/2005

FROMMER LAWRENCE & HAUG
745 FIFTH AVENUE- 10TH FL.
NEW YORK, NY 10151

EXAMINER
LEMMA, SAMSON B

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 06/06/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _28 February 2005_.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-3,5-13,15-28 and 31-44_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-3,5-13,15-28 and 31-44_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.
5)☐ Notice of Informal Patent Application (PTO-152)
6)☐ Other: _____.

DETAILED ACTION

1.   This office action is in replay to an amendment filed on February 28, 2005.

Claims 1, 5-7, 11, 15-17, 21-24 and 26 have been amended. **Claims 4 and**

14 are cancelled and claims **29 and 30** have previously been cancelled. Applicant

has added new claims **40-44. Claims 1-3, 5-13,15-28, and 31-44** are pending.

Response to Arguments

2.   Applicant's arguments with respect to **Claims 1, 5-7, 11, 15-17, 21-24 and 26**

have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

3.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for

all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or
> described as set forth in section 102 of this title, if the differences between the subject
> matter sought to be patented and the prior art are such that the subject matter as a
> whole would have been obvious at the time the invention was made to a person having
> ordinary skill in the art to which said subject matter pertains. Patentability shall not be
> negatived by the manner in which the invention was made.

4.   **Claims 1,5-28,31-43** are rejected under 35 U.S.C. 103(a) as being

unpatentable over, Chung et al (hereinafter referred as Chung)(U.S. Patent 6,310,962)

in view of "Linnartz". (hereinafter referred to as Linnartz) (U.S. Patent No. 6,314,518)

further in view of Hayashi et al. (hereinafter referred to as Hayashi) (U.S.Publication No.

2003/0161496 A1)

5.   **As per claims 1, 11 ,27 and 28** Chung discloses a material processing

system/computer program for processing material including a watermark, the system

comprising (the "material" is met by the applicant as e.g. video, audio or data on the

submitted abstract on the first sentence and on the submitted diagram, figure 1, ref.

Num "632". The office has interpreted the "material" in light of the disclosure)

- A remover for removing the watermark, (figure 6, ref. Num

"224";figure 7, ref. Num "270" ; Column 8, lines 65-Column 9, line 3;

column 9, lines 45-50)

- A processor for processing the material from which the watermark

has been removed,(figure 6, ref. Num " 224"; Column 8, lines 65-column

9, line 3) (The "processor" is defined by the applicant as editor a special

effect machine, a mixer or any other video processor as explained on the

submitted disclosure page 3, lines 5-7. The office has interpreted the

processor as the "adaptive estimator" for video processing which is used

for preventing the error during the motion estimation by first removing

the digital watermark information and process the encoded data without

the watermark information as explained on column 8, lines 65- column 9

line 3 and shown on figure 6, ref. Num "230")

- An inserter for inserting a watermark into the processed material.

(Figure 6, ref. Num "240"; figure 7, ref. Num "272"; column 8, lines 35-

59) (The digital data which the watermark has been removed from by the

digital watermark remover is processed by the adaptive estimator and

then the digital watermark is inserted again on the processed encoded

data as shown on figure 6, ref. Num "240". Figure 7, ref. Num "272" also

shows how the digital watermark is re-inserted once it has been

removed.)

Chung does not explicitly disclose a system according to claim 1, and 11 further comprising a database processor linked to the remover, the database processor containing data enabling the removal of the watermark from the material to be processed.

However, in the same field of endeavor, **Linnartz** discloses a detector as shown on figure 6, ref. Num "69" able to detect or retrieve or remove the watermark information from the digital data and send it back to the controller in the drive as shown on figure 6, ref. NUM "52" after the digital data is decrypted by retrieving the key which is shown on figure 6, ref. Num "65" at the decryption unit or key storage unit as shown on figure 6, ref. Num "66". The drive as shown on figure 6, ref. Num "52" first encrypt the digital data which has a watermark information in it with the encryption key shown on figure 6, ref. Num "62" stored at the unit shown on figure 6, ref. Num "61" and sent the encrypted digital data through a secure path shown on figure 6, ref. Num "63". The decoder has a storage unit as shown on figure 6, ref. Num "66" which stores the decryption key as shown on figure 6, ref. Num "65". The detector shown on figure 6, ref. Num "69" using this key accessed from the storage unit, retrieves or removes the watermark information and encrypt this watermark information at the encryption unit as shown on figure 6, ref. Num "67" and send to the controller shown on figure 6, ref. Num "53",via secure path shown on the figure 6, ref. Num "64". The controller controllers the processing of the material based on this watermark information. (Column 8, lines 31-56)

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features of accessing the enabling data or encryption/decryption key from the key store to retrieve or detect or removes the watermark information which is embedded in the digital data as per

teachings of Linnartz in to the method taught by Chung, in order to securely remove the watermark and communicate the watermark to controller so that the watermark information is not damaged during processing and prevent illegally accessing or changing of the watermark information by unauthorized users.

The combination of Chung and Linnartz does not explicitly disclose combining the watermark code **with predetermined components** of the material and the removal of the watermark from the material to be processed, the enabling data **indicating the predetermined component** of the material with which the watermark code word has been combined.

However, in the same field of endeavor, **Hayashi** discloses the watermark embedding means for embedding a watermark information at **a predetermined component of the material in coefficient having values falling within a predetermined range of the input image data**. [page 1, ref. Num "0022"] and the enabling data or the information necessary for extraction /removal of watermark is sent to the watermark extracting/removing device shown on figure 2, ref. Num "203". This enabling data indicates the predetermined component of the material with which the watermark code has been combined. The digital-watermark extracting device shown on figure 2, ref. Num "203" extracts the information indicating the predetermined component of the material with which the watermark is combined and be able to extract/remove the watermark.[column 4, ref. Num "0102", ref. Num "0107"0108" and figure 1, figure 2 and abstract]

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features of combining the watermark with **the predetermined component of the material** and to provide the remover /watermark extractor with the enabling data or information necessary

for the extraction of the predetermined component of the material with which

the watermark is combined as per teachings of Hayashi in to the method of

removing watermark information as taught by the combination of **chung and**

Linnartz in order to reliably extract the digital-watermark information.[See

Hayashi page 1, ref. Num "0018"]

6.   **As per claims 12 and 13** the combination of **Chung, linnartz and Hayashi**

discloses the method as applied to claim 11 above. Furthermore Chung discloses the

method wherein the steps of removing and inserting are automatic and independent of

a user of the processor and are also hidden from the user. (figure 6, ref. Num "240" and

ref. Num "242"; figure 7, ref. Num "270" and ref. Num "272"; column 9, lines 37)

7.   **As per claims 21-24 and 40** **Chung** discloses

- A method of removing data embedded in material (figure 6, ref. Num

"242" and figure 7, ref. Num "270"; Column 8, lines 65-Column 9, line 3; column 9,

lines 45-50) (the "data embedded in material" is met by the applicant and the office as

the "watermark " as explained on the submitted disclosure on pages 1 and 2)

comprising the steps of:

- Receiving material in which data is embedded; (figure 6, ref. Num "242", figure

7, ref. Num "272") (the digital data with the watermark embedded in it is received at the

digital watermark remover as shown on figure 6, ref. Num "242" and figure 7, ref. Num "

242" from the "dequantizer" as shown on figure 6 and 7 respectively.)

Furthermore Nakano discloses how the watermark is intentionally removed at

the digital watermark remover. (Figure 6, ref. Num "242" and figure 7, ref. Num "270")

Chung does not explicitly disclose accessing an information store storing information

enabling the data to be removed; and removing the said data using the enabling data

accessed from the store. (The "enabling data" is defined by the applicant as "encryption
/decryption key" as explained on page 1, line 24, the same interpretation is used by the
office).

However, in the same field of endeavor, **Linnartz** discloses a detector as shown on
figure 6, ref. Num "69" able to detect or retrieve or remove the watermark information
from the digital data and send it back to the controller in the drive as shown on figure
6, ref. NUM "52" after the digital data is decrypted by retrieving the key which is shown
on figure 6, ref. Num "65" at the decryption unit or key storage unit as shown on figure
6, ref. Num "66". The drive as shown on figure 6, ref. Num "52" first encrypt the digital
data which has a watermark information in it with the encryption key shown on figure
6, ref. Num "62" stored at the unit shown on figure 6, ref. Num "61" and sent the
encrypted digital data through a secure path shown on figure 6, ref. Num "63". The
decoder has a storage unit as shown on figure 6, ref. Num "66" which stores the
decryption key as shown on figure 6, ref. Num "65". The detector shown on figure 6, ref.
Num "69" using this key accessed from the storage unit, retrieves or removes the
watermark information and encrypt this watermark information at the encryption unit
as shown on figure 6, ref. Num "67" and send to the controller shown on figure 6, ref.
Num "53",via secure path shown on the figure 6, ref. Num "64". The controller
controllers the processing of the material based on this watermark information.
(Column 8, lines 31-56)

> It would have been obvious to one having ordinary skill in the art, at the time
> the invention was made, to combine the features of accessing the enabling data
> or encryption/decryption key from the key store to retrieve or detect or removes
> the watermark information which is embedded in the digital data as per
> teachings of Linnartz in to the method taught by Chung, in order to securely
> remove the watermark and communicate the watermark to controller so that the

watermark information is not damaged during processing and prevent illegally

accessing or changing of the watermark information by unauthorized users.

The combination of Chung and Linnartz does not explicitly disclose combining

the watermark code with predetermined components of the material and the

removal of the watermark from the material to be processed, the enabling data

indicating the predetermined component of the material with which the

watermark code word has been combined.

However, in the same field of endeavor, **Hayashi** discloses the watermark

embedding means for embedding a watermark information at a predetermined

component of the material in coefficient having values falling within a

predetermined range of the input image data. [page 1, ref. Num "0022"; abstract]

and the enabling data or the information necessary for extraction /removal of

watermark is sent to the watermark extracting/removing device shown on figure

2, ref. Num "203". This enabling data indicates the predetermined component of

the material with which the watermark code has been combined. The digital-

watermark extracting device shown on figure 2, ref. Num "203" extracts the

information indicating the predetermined component of the material with which

the watermark is combined and be able to extract/remove the watermark.[

column 4, ref. Num "0102", ref. Num "0107"0108" and figure 1, figure 2 and

abstract]

It would have been obvious to one having ordinary skill in the art, at the time

the invention was made, to combine the features of combining the watermark

with the predetermined component of the material and to provide the remover

/watermark extractor with the enabling data or information necessary for the

extraction of the predetermined component of the material with which the

watermark is combined as per teachings of Hayashi in to the method of

removing watermark information as taught by the combination of chung and

Linnartz in order to reliably extract the digital-watermark information.[See

Hayashi page 1, ref. Num "0018"]

8.   **As per claims 5 and 15**, **Chung** discloses the method of removing watermark

information and later inserting the watermark information as shown on figure 6, ref.

Num "242" and ref. Num "240" or figure 7, ref. Num "270" and ref. Num "272").

Chung does not explicitly disclose a database processor linked to the inserter, the

database processor containing data enabling insertion of the watermark into the

processed material. (The "enabling data" is defined by the applicant as "encryption

/decryption key" as explained on page 1, line 24, the same interpretation is used by the

office).

However, in the same field of endeavor, **Linnartz** discloses a decoder and a drive which

are communicating the watermark information through a secure link by using

encryption/decryption key as shown on figure 6, ref. Num "62" and ref. Num "65" which

is stored in the encryption/decryption unit as shown on figure 6, ref. Num "61" and ref.

Num "66" respectively which is interpreted by the office as the database for storing

keys.(figure 6; column 8, lines 31-56)

It would have been obvious to one having ordinary skill in the art, at the time the

invention was made, to combine the features of accessing and transmitting watermark

information using encryption/decryption key from the key store or database to access

or retrieve the watermark information as per teachings of Linnartz in to the method

taught by Chung, in order to securely insert the watermark and prevent illegally

accessing or changing of the watermark information by unauthorized users. Therefore,

what has been disclosed above by the combination of Chung, linnartz and Hayashi

meets the recitation of the claims 5 and 15.

9.   **As per claims 9 and 19**, **Chung** discloses two ways of preventing illegal copying

one method is using encryption and the other method is using watermark method. The

watermark is embedding or inserting to prevent illegal copying. (Column 1, lines 43-62).

Furthermore Chung discloses that the watermark is used on the original image and is

invisible to unauthorized users but the author can prove that the copied image is his by

virtue of an arbitrary reverse processing. (Column 1, lines 59-62)

Chung does not explicitly disclose the system arranged to check the authenticity of the

said material including the reversible watermark.

However, in the same field of endeavor, **Linnartz** discloses using the drives hashes and

adds random number and signs the MPEG stream using the well known cryptographic

algorithms like RSA or DSA. The MPEG decoder then verifies the signature and detects

the watermark and sends the message back to the drive. (Column 8, lines 65-column 9,

line 1).

It would have been obvious to one having ordinary skill in the art, at the time the

invention was made, to combine the features of checking the authenticity of the

communicating parities transferring and receiving digital data using hashes and digital

signature as per teachings of Linnartz in to the method taught by Chung, in order to

authenticate the digital data or the material on which the watermark is embedded.

Therefore, what has been disclosed above by the combination of Chung, linnartz and

Hayashi meets the recitation of the claims 9 and 19.

10.   **As per claims 6, 16, 31 and 34**, the combination of Chung, Linnartz and

Hayashi discloses the methods as applied to claims 1, 11, 5 and 15 above. Furthermore

Linnartz discloses the system/ method/ apparatus further wherein the said enabling

data includes an encryption key. (figure 6, ref. Num "62"; column 8, lines 31-56)

11.   **As per claims 7, 17, 32, and 35**, the combination of Chung, Linnartz and

Hayashi discloses the methods as applied to claims 1, 11, 5 and 15 above. Furthermore

Linnartz discloses the system/ method/ apparatus wherein the inserter and the

remover are linked to the database processor by a communications link.(figure 6, ref.

Num "64")

12.   **As per claims 8, 18, 36**, the combination of Chung, Linnartz and **Hayashi**

discloses the methods as applied to claims 7, 17 and 35 above. Furthermore Linnartz

discloses the system/ method/ apparatus wherein the communications link includes

the internet. (Column 9, lines 53-58)

13.   **As per 33**, the combination of Chung, Linnartz and **Hayashi** discloses the

methods as applied to claims 8 above. Furthermore Linnartz discloses the system/

method/ apparatus wherein the inserter and the remover are linked to the database

processor by a communications link. (figure 6, ref. Num "64")

14.   **As per claims 10, 20 and 41-42** the combination of Chung, Linnartz and

Hayashi discloses the methods as applied to claims 9 and 19 above. Furthermore

Linnartz discloses the system/ method/ apparatus wherein arranged to disable the said

processor if the material fails the authenticity check. (Column 8, lines 57-67)

15.   **As per claim 25,** the combination of Chung, Linnartz and **Hayashi** discloses the

methods as applied to claims 23 above. Furthermore Linnartz discloses an apparatus

wherein a generator for generating the enabling information. (Figure 6, ref. Num "61" ,

figure 6, ref. Num "66" and figure 6, ref. Num "67" and "60") (The "enabling data" is

defined by the applicant as "encryption /decryption key" as explained on page 1, line

24, the same interpretation is used by the office. These keys are generated/available

and stored wherever the encryption and decryption is performed as explained on

column 8, lines 31-57).

16.   **As per claims 26, 37-39 and 43**, the combination of Chung, Linnartz and

Hayashi discloses the methods as applied to claims 24,21,22,1 above. Furthermore

Chung discloses an apparatus wherein the material is one or more of video material,

audio material and data material. (Figure 1, ref "Video Input")

17.   **Claims 2 and 3** are rejected under 35 U.S.C. 103(a) as being unpatentable over,

Chung et al (hereinafter referred as Chung)(U.S. Patent 6,310,962) in view of "Linnartz".

(hereinafter referred to as Linnartz) (U.S. Patent No. 6,314,518) further in view of

Hayashi et al. (hereinafter referred to as Hayashi) (U.S.Publication No. 2003/0161496

A1) further in view of Nakano, Hirotaka. (hereinafter referred to as Nakano) (European

patent application publication). (EP 0859503 A2)

18.   **As per claim 2, the combination of** Chung, Linnartz and Hayashi discloses that

the digital watermark inserter as shown on figure 6, ref. Num "240" makes digital

watermark information not removable by a user except an author or authorized

user.(column 8, lines 11-12).

The combination of Chung, Linnartz and Hayashi does not explicitly disclose the

processor has a user interface for controlling the processes performed thereby.

However, in the same field of endeavor, **Nakano** discloses authorized users accessing

the watermark information produced by the processor by interfacing with data

communication controller as shown on figure 6, ref. Num "604". (Column 6, line 50-column 7, line 24)

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features of proving authorized user interface for accessing the watermark produced by the processor through the controller as per teachings of **Nakano** in to the method taught by the combination of Chung, Linnartz and Hayashi in order to provide authorized user to directly access the corresponding watermark information.

19.   **As per claims 3,** the combinations of chung, Linnartz, Hayashi and Nakano discloses the system as applied to claims 2 and above. Furthermore Chung discloses the system wherein the remover and the inserter are arranged to operate automatically and independently of the user. (figure 6, ref. Num "240" and ref. Num "242"; figure 7, ref. Num "270" and ref. Num "272"; column 9, lines 37)

Conclusion

20.   Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Samson B Lemma whose telephone number is 571-272-

3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).
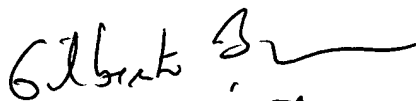
If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone

number for the organization where this application or proceeding is assigned is 703-

872-9306.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published

applications may be obtained from either Private PAIR or Public PAIR. Status

information for unpublished applications is available through Private PAIR only. For

more information about the PAIR system, see http://pair-direct.uspto.gov. Should you

have questions on access to the Private PAIR system, contact the Electronic Business

Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA

S.L.

May 10, 2005

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100